GOVERNMENT OF INDIA
ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA

UNSTARRED QUESTION NO:1084
ANSWERED ON:08.02.2017
Cyber Attack and Hacking
Diwakar Shri Rajesh Kumar;Gandhi Dr. Dharam Vira;Kaswan Shri Rahul;Mahtab Shri Bhartruhari;Patel Shri Prahlad Singh;Solanki Dr. Kirit Premjibhai;Udasi Shri Shivkumar Chanabasappa;Vanaroja Smt. R.

Will the Minister of ELECTRONICS AND INFORMATION TECHNOLOGY be pleased to state:

Will the Minister of Electronics & Information Technology be pleased to state:-
(a) whether the instances of cyber attack and hacking of Indian websites from foreign countries have increased during each of the last three years and the current year;
(b) if so, the details thereof, country-wise and the reasons therefor;
(c) whether the Government has taken up the issue of hacking of Indian websites with the respective country under bilateral cooperation;
(d) if so, the details and the outcome thereof and if not, the reasons therefor;
(e) whether the Government and the Government offices are equipped with standard information security measures to restrict unauthorized access to official information by the hackers and comply with IPv6 internet protocol system and if so, the details thereof; and
(f) whether the Government has taken/will be taking measures to regulate social media to restrict circulation of anti-social and anti-India information from terrorist outfits and if so, the details thereof?

Answer

(a) and (b): As per the information reported to and tracked by Indian Computer Emergency Response Team (CERT-In) a total number of 28481, 32323, 27205 and 33147 websites were hacked during the year 2013, 2014, 2015 and 2016 respectively. With the increase in the proliferation of Information Technology and mobile applications and related services, there is rise in the incidents of cyber attacks in the past years. Similar trend is observed worldwide also. The hackers are exploiting vulnerabilities in the hardware and software associated with web applications. It has been observed attacks are launched through compromised computer systems located in different parts of the world. Masquerading techniques and hidden servers are also used to hide the identity of the actual systems being used by malicious actors. The attacks are observed to be originating from various countries including China, Germany, Hong Kong, Japan, Malaysia, Pakistan, Romania, United Kingdom, United States of America, Syria, United Arab Emirates and Italy. Affected organisations are notified with remedial measures to mitigate vulnerabilities and secure their respective websites..

(c) and (d): Memorandum of Understanding (MoU) have been signed between CERT-In and Computer Emergency Response Teams (CERTs) in other countries for enhancing bilateral cooperation in the area of cyber security for effective resolution of cyber security incidents and mitigation of cyber attacks. CERT-In coordinates with its counterpart agencies in respective countries for mitigation of incidents involving systems outside the country.

(e) In order to prevent unauthorised access and secure Information Technology infrastructure, the following measures have been taken:

i. National Informatics Centre (NIC) which provides Information Technology related services to Government Departments, publishes cyber security policies, procedures, guidelines and advisories in the security portal for its users.

ii. CERT-In publishes guidelines regularly for securing the websites, computer systems and applications, which are available on its website (www.cert-in.org.in).
iii. Government (MeitY) has formulated Cyber Crisis Management Plan (CCMP) for countering cyber attacks and cyber terrorism for implementation by all Ministries/ Departments of Central Government, State Governments and their organizations and critical sectors. 42 workshops have been conducted for Ministries/Departments, States & Union Territories and critical organizations to sensitise them about the cyber security threat landscape and enabling them to prepare and implement the Cyber Crisis Management Plan.
iv. NIC protects the cyber resources from possible compromises through a layered security approach in the form of practices, procedures and technologies that are put in place. NIC has deployed state-of-the-art security solutions including firewalls, intrusion prevention systems, anti-virus solution. Additionally, periodic security audits of resources are performed followed by subsequent hardenings. These are complemented by round-the-clock monitoring of security events and remedial measures are carried out for solving the problems subsequently. Networking equipments installed in Government Buildings by NIC/ or under guidance of NIC comply with IPv6.
v. National Critical Information Infrastructure Protection Centre (NCIIPC) is also engaged with Chief Information Security Officers (CISOs) of various Government offices (Central & States) and sending alerts and advisories for the protection of critical information infrastructure periodically.
vi. Government (MeitY) is also supporting a project titled 'IPv6 Training Programme for Staff of Government/ Ministries & Institution' to enhance adoption and deployment of IPv6 and the project is being implemented by ERNET India. Under this project, ERNET India has setup an Infrastructure in line with the one hosted by APNIC at 3 locations i.e Delhi, Chennai and Bangalore. These infrastructures are available over the Internet and hands-on training and live experience have been provided to about 500 network related participants

from Government sector at various cities i.e. Delhi, Chennai, Chandigarh, Puducherry, Bhopal and Kolkata.

vii. Department of Telecom (DoT) has mandated that the licensee (including BSNL & MTNL) shall induct only those network elements into their telecom network, which have been got tested as per relevant contemporary Indian or international security standards which also include information security management system against ISO 27000 series standards. Moreover, DoT has also advised its sub-ordinate departments/organizations to adhere with policy guidelines on cyber security i.e. 'National Information Security Policy and Guidelines' and 'Cyber Security Policy'. DoT has asked the Central Government Ministries/Departments, State and Union Territories government for transition to IPv6 in accordance with "National IPv6 Deployment Roadmap v-II" guidelines. The Government organizations have been asked to align and integrate the IPv6 transition of their networks with the product/technology life cycles to reduce the capital expenditure and do the transition by December 2017. DoT has issued guidelines to Government organizations that all new ICT equipment to be procured should be IPv6 ready.

(f): The Social Media is being made use of by the citizens across world through Internet. Government does not regulate the content appearing on social networking sites. However, at times these services are also used by anti-national/anti-social elements, which pose a security threat. The Information Technology (IT) Act, 2000 has provisions for removal of objectionable online content. The Information Technology (Intermediary Guidelines) Rules 2011 under section 79 of the IT Act requires that the Intermediaries shall observe due diligence while discharging their duties and shall inform the users of computer resources not to host, display, upload, modify, publish, transmit, update or share any information that is harmful, objectionable, affect minors and unlawful in any way. Further, Government takes action under section 69A of IT Act for blocking of websites/webpages with objectionable contents, whenever requests are received from designated nodal officers or upon Court orders. Section 69A of the IT Act empowers Government to block any information generated, transmitted, received, stored or hosted in any computer resource in the interest of i) sovereignty and integrity of India, ii) defence of India, iii) security of the State, iv) friendly relations with foreign States v) public order or vi) for preventing incitement to the commission of any cognizable offence relating to above.

The Government has also mandated all the Telecom Service Providers including Internet Service Providers to provide the Lawful Interception facilities to the security agencies for all the services including WhatsApp, Viber, etc. As such Security agencies are able to intercept these encrypted communication services through the lawful interception facilities provided by the Telecom Service Providers, but they are not able to decrypt some of encrypted intercepted communication to readable format.

*****